

Amendments to the Claims

1 Claim 1 (currently amended): In a computing environment having a connection to a network, a
2 computer program product for securely propagating security credentials using a trusted
3 authenticating domain, the computer program product embodied on one or more computer-
4 readable media and comprising:

5 computer-readable program code means for establishing a secure connection between a
6 client and a password synchronization agent (PSA);

7 computer-readable program code means for transmitting an identifier of a user and an
8 identifying secret of the user from the client to the PSA over the secure connection;

9 computer-readable program code means for validating the user with the trusted
10 authenticating domain using the transmitted user identifier and identifying secret, on request of the
11 PSA; and

12 computer-readable program code means for propagating the identifying secret of the user
13 directly from the PSA to a master registry if the validation succeeds.

1 Claim 2 (original): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for establishing a second secure connection
3 between the PSA and the trusted authenticating domain; and

4 computer-readable program code means for using the second secure connection for the
5 validating of the user.

1 Claim 3 (original): The computer program product according to Claim 1, further comprising:

Serial No. 09/614,087

-5-

Docket RSW9-2000-0074-US1

2 computer-readable program code means for establishing a third secure connection
3 between the PSA and the master registry; and

4 computer-readable program code means for using the third secure connection for the
5 propagating of the identifying secret to the master registry.

1 Claim 4 (original): The computer program product according to Claim 1, further comprising
2 computer-readable program code means for propagating the identifying secret to one or more
3 other target registries if the validation succeeds.

1 Claim 5 (original): The computer program product according to Claim 4, further comprising:

2 computer-readable program code means for establishing additional secure connections
3 between the PSA and each of the other target registries; and

4 computer-readable program code means for using the additional secure connections for
5 the propagating of the identifying secret to the other target registries.

1 Claim 6 (original): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for obtaining an identification of the trusted
3 authenticating domain from the user; and

4 computer-readable program code means for verifying that the trusted authenticating
5 domain is trusted by the master registry as a prerequisite to the propagating.

1 Claim 7 (original): The computer program product according to Claim 1, further comprising:

Serial No. 09/614,087

-6-

Docket RSW9-2000-0074-US1

2 computer-readable program code means for obtaining an identification of the trusted
3 authenticating domain from the master registry.

1 Claim 8 (original): The computer program product according to Claim 6, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for verifying that the trusted authenticating domain is trusted further comprises computer-readable
4 program code means for checking whether the stored trust policy information for the user
5 includes the identification obtained from the user.

as
1 Claim 9 (original): The computer program product according to Claim 6, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for verifying that the trusted authenticating domain is trusted further comprises computer-readable
4 program code means for checking whether the stored trust policy information for a user group of
5 which the user is a member includes the identification obtained from the user.

1 Claim 10 (original): The computer program product according to Claim 7, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for obtaining the identification of the trusted authenticating domain from the master registry
4 further comprises computer-readable program code means for obtaining the identification using
5 the stored trust policy information for the user.

1 Claim 11 (original): The computer program product according to Claim 7, wherein the master

Serial No. 09/614,087

-7-

Docket RSW9-2000-0074-US1

2 registry stores trust policy information, and wherein the computer-readable program code means
3 for obtaining the identification of the trusted authenticating domain from the master registry
4 further comprises computer-readable program code means for obtaining the identification using
5 the stored trust policy information for a user group of which the user is a member.

1 Claim 12 (original): The computer program product according to Claim 4, wherein the master
2 registry stores password synchronization policy information, and wherein the computer-readable
3 program code means for propagating the identifying secret to the one or more other target
4 registries further comprises computer-readable program code means for identifying the one or
5 more other target registries using the stored password synchronization policy information for the
6 user.

1 Claim 13 (original): The computer program product according to Claim 4, wherein the master
2 registry stores password synchronization policy information, and wherein the computer-readable
3 program code means for propagating the identifying secret to the one or more other target
4 registries further comprises computer-readable program code means for identifying the one or
5 more other target registries using the stored password synchronization policy information for a
6 user group of which the user is a member.

1 Claim 14 (original): The computer program product according to Claim 1, wherein the computer-
2 readable program code means for establishing the secure connection further comprises computer-
3 readable program code means for authenticating the PSA to the client.

Serial No. 09/614,087

-8-

Docket RSW9-2000-0074-US1

1 Claim 15 (original): The computer program product according to Claim 2, wherein the computer-
2 readable program code means for establishing the second secure connection further comprises
3 computer-readable program code means for authenticating the trusted authenticating domain to
4 the PSA.

1 Claim 16 (original): The computer program product according to Claim 3, wherein the computer-
2 readable program code means for establishing the third secure connection further comprises
3 computer-readable program code means for authenticating the master registry to the PSA.

as

1 Claim 17 (original): The computer program product according to Claim 5, wherein the computer-
2 readable program code means for establishing additional secure connections further comprises
3 computer-readable program code means for authenticating the other target registries to the PSA.

1 Claim 18 (currently amended): The computer program product according to Claim 1, wherein the
2 computer-readable program code means for validating further comprises:

3 computer-readable program code means for performing a security function on the
4 identifying secret of the user, wherein the security function comprises one of (i) a one-way
5 hashing algorithm or (ii) an encryption algorithm;

6 computer-readable program code means for using the user identifier to locate a
7 previously-stored identifying secret of the user which was stored by the trusted authenticating
8 domain; and

Serial No. 09/614,087

-9-

Docket RSW9-2000-0074-US1

9 computer-readable program code means for concluding that the validation succeeds if
10 comparing the located identifying secret is identical to a result of performing the security function.

1 Claim 19 (original): The computer program product according to Claim 1, wherein the computer-
2 readable program code means for validating further comprises computer-readable program code
3 means for invoking an authenticated LDAP bind or other native authentication mechanism of the
4 trusted authenticating domain, wherein the identifier of the user and the identifying secret of the
5 user are passed to the trusted authenticating domain, thereby causing the trusted authenticating
6 domain to validate the passed identifier and identifying secret and return a result which reports a
7 success or failure of the validation.

1 Claim 20 (original): The computer program product according to Claim 1, wherein the PSA has
2 administrative authority for performing operations at the master registry.

1 Claim 21 (original): The computer program product according to Claim 4, wherein the PSA has
2 administrative authority for performing operations at the one or more other target registries.

1 Claim 22 (currently amended): A system for securely propagating security credentials using a
2 trusted authenticating domain, comprising:

3 means for establishing a secure connection between a client and a password
4 synchronization agent (PSA);

5 means for transmitting an identifier of a user and an identifying secret of the user from the

Serial No. 09/614,087

-10-

Docket RSW9-2000-0074-US1

6 client to the PSA over the secure connection:

7 means for validating the user with the trusted authenticating domain using the transmitted
8 user identifier and identifying secret, on request of the PSA; and

9 means for propagating the identifying secret of the user directly from the PSA to a master
10 registry if the validation succeeds.

1 Claim 23 (original): The system according to Claim 22, further comprising:

2 means for establishing a second secure connection between the PSA and the trusted
3 authenticating domain; and

4 means for using the second secure connection for the validating of the user.

1 Claim 24 (original): The system according to Claim 22, further comprising:

2 means for establishing a third secure connection between the PSA and the master registry;
3 and

4 means for using the third secure connection for the propagating of the identifying secret to
5 the master registry.

1 Claim 25 (original): The system according to Claim 22, further comprising means for propagating
2 the identifying secret to one or more other target registries if the validation succeeds.

1 Claim 26 (original): The system according to Claim 25, further comprising:

2 means for establishing additional secure connections between the PSA and each of the

Serial No. 09/614,087

-11-

Docket RSW9-2000-0074-US1

3 other target registries; and
4 means for using the additional secure connections for the propagating of the identifying
5 secret to the other target registries.

1 Claim 27 (original): The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the user;
3 and
4 means for verifying that the trusted authenticating domain is trusted by the master registry
5 as a prerequisite to the propagating.

as

1 Claim 28 (original): The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the master
3 registry.

1 Claim 29 (original): The system according to Claim 27, wherein the master registry stores trust
2 policy information, and wherein the means for verifying that the trusted authenticating domain is
3 trusted further comprises means for checking whether the stored trust policy information for the
4 user includes the identification obtained from the user.

1 Claim 30 (original): The system according to Claim 27, wherein the master registry stores trust
2 policy information, and wherein the means for verifying that the trusted authenticating domain is
3 trusted further comprises means for checking whether the stored trust policy information for a

Serial No. 09/614,087

-12-

Docket RSW9-2000-0074-US1

4 user group of which the user is a member includes the identification obtained from the user.

1 Claim 31 (original): The system according to Claim 28, wherein the master registry stores trust
2 policy information, and wherein the means for obtaining the identification of the trusted
3 authenticating domain from the master registry further comprises means for obtaining the
4 identification using the stored trust policy information for the user.

1 Claim 32 (original): The system according to Claim 28, wherein the master registry stores trust
2 policy information, and wherein the means for obtaining the identification of the trusted
3 authenticating domain from the master registry further comprises means for obtaining the
4 identification using the stored trust policy information for a user group of which the user is a
5 member.

1 Claim 33 (original): The system according to Claim 25, wherein the master registry stores
2 password synchronization policy information, and wherein the means for propagating the
3 identifying secret to the one or more other target registries further comprises means for
4 identifying the one or more other target registries using the stored password synchronization
5 policy information for the user.

1 Claim 34 (original): The system according to Claim 25, wherein the master registry stores
2 password synchronization policy information, and wherein the means for propagating the
3 identifying secret to the one or more other target registries further comprises means for

Serial No. 09/614,087

-13-

Docket RSW9-2000-0074-US1

4 identifying the one or more other target registries using the stored password synchronization
5 policy information for a user group of which the user is a member.

1 Claim 35 (original): The system according to Claim 22, wherein the means for establishing the
2 secure connection further comprises means for authenticating the PSA to the client.

1 Claim 36 (original): The system according to Claim 23, wherein the means for establishing the
2 second secure connection further comprises means for authenticating the trusted authenticating
3 domain to the PSA.

as
1 Claim 37 (original): The system according to Claim 24, wherein the means for establishing the
2 third secure connection further comprises means for authenticating the master registry to the PSA.

1 Claim 38 (original): The system according to Claim 26, wherein the means for establishing
2 additional secure connections further comprises means for authenticating the other target
3 registries to the PSA.

1 Claim 39 (currently amended): The system according to Claim 22, wherein the means for
2 validating further comprises:
3 means for performing a security function on the identifying secret of the user, wherein the
4 security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;
5 means for using the user identifier to locate a previously-stored identifying secret of the

Serial No. 09/614,087

-14-

Docket RSW9-2000-0074-US1

6 user which was stored by the trusted authenticating domain; and

7 means for concluding that the validation succeeds if comparing the located identifying
8 secret is identical to a result of performing the security function.

1 Claim 40 (original): The system according to Claim 22, wherein the means for validating further
2 comprises means for invoking an authenticated LDAP bind or other native authentication
3 mechanism of the trusted authenticating domain, wherein the identifier of the user and the
4 identifying secret of the user are passed to the trusted authenticating domain, thereby causing the
5 trusted authenticating domain to validate the passed identifier and identifying secret and return a
6 result which reports a success or failure of the validation.

1 Claim 41 (original): The system according to Claim 22, wherein the PSA has administrative
2 authority for performing operations at the master registry.

1 Claim 42 (original): The system according to Claim 25, wherein the PSA has administrative
2 authority for performing operations at the one or more other target registries.

1 Claim 43 (currently amended): A method for securely propagating security credentials using a
2 trusted authenticating domain, comprising steps of:

3 establishing a secure connection between a client and a password synchronization agent

4 (PSA);

5 transmitting an identifier of a user and an identifying secret of the user from the client to

Serial No. 09/614,087

-15-

Docket RSW9-2000-0074-US1

6 the PSA over the secure connection;

7 validating the user with the trusted authenticating domain using the transmitted user
8 identifier and identifying secret, on request of the PSA; and

9 propagating the identifying secret of the user directly from the PSA to a master registry if
10 the validation succeeds.

1 Claim 44 (new): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for obtaining a new value fro the user to be used
3 as the propagated identifying secret if the validation succeeds; and

4 computer-readable program code means for substituting this new value for the identifying
5 secret prior to operation of the computer-readable program code means for propagating.

1 Claim 45 (new): The system according to Claim 22, further comprising:

2 means for obtaining a new value fro the user to be used as the propagated identifying
3 secret if the validation succeeds; and

4 means for substituting this new value for the identifying secret prior to operation of the
5 means for propagating.

1 Claim 46 (new): The method according to Claim 43, further comprising steps of:

2 obtaining a new value fro the user to be used as the propagated identifying secret if the
3 validation succeeds; and

4 substituting this new value for the identifying secret prior to operation of the propagating

Serial No. 09/614,087

-16-

Docket RSW9-2000-0074-US1

5 step.

as

Serial No. 09/614,087

-17-

Docket RSW9-2000-0074-US1